Crime Mapping and Data Confidentiality Roundtable July 8-9, 1999

Sponsored by: National Institute of Justice, Crime Mapping Research Center

Balancing Public and Private Rights in Mapping Crime: Two Axioms to Guide Our Thinking

by
David Anderson,
Director of Community Programs,
National Center for Victims of Crime

Introduction

The balance point between the public's right to know and a crime victim's right to privacy is like the fulcrum on a see-saw. Just as a see-saw can be adjusted to accommodate children of different sizes, the balance point between the right to know and the right to privacy can be changed to achieve a theoretically optimal benefit. While technologies like computer mapping can create tremendous benefits for everyone, they can also shift the balance point too far to the side of public benefit, thereby causing private harm.

To prevent this, we need to answer some fundamental questions. When should the needs of the one be subsumed by the needs of the many? Alternatively, when should we allow a public risk so that we may protect the privacy of an individual? How should these decisions be made? Should computerized crime maps provide all legally available information about crime victims or does the comprehensive nature of computer mapping make it necessary to degrade certain types of data (depending on the users of that data)? Should victim privacy statutes be amended to define the types of information that can and cannot be depicted in computer mapping?

Victim Privacy Overview

At the National Center for Victims of Crime, we believe that a crime victim's right to privacy is very important. Fear of harassment or retaliation deters many victims from seeking justice. Others, not wanting the world to know what has happened to them, refuse to report crimes to protect their privacy. Victims who believe that their privacy is not being respected may be less likely to cooperate with the investigation and prosecution of their case. Quite often, the irresponsible release of confidential information can place a victim of crime in danger. Ultimately, provisions that protect the privacy of crime victims are crucial to helping victims regain a sense of security.

Most jurisdictions provide statutory protections for a victim's right to privacy. The specific elements of victim-related information most often protected from disclosure include address, phone number, place of employment, and identity. Some jurisdictions extend this protection to witnesses or the immediate members of the victim's family. However, these protections vary greatly by jurisdiction and may not take into account the tremendous information gathering potential of computer technology.

Axioms for the Protection and Disclosure of Information

The optimal balance point between the public right to know and the privacy of crime victims depends on the type of crime, the type of victim, and community standards. In addition, the decision about what information is protected and what information is disclosed should also be based on the medium of disclosure. It is one thing to allow access to particular information upon request, but quite another to publish information on a web site or on material to be publicly distributed. While statutes should determine the minimum standards, policies should establish tighter restrictions when appropriate.

Two Axioms

Axiom 1: Do no harm. The control of information should be proportional to the potential harm it's release could cause to a victim.

Axiom 2: The detail of the information provided should be proportional to the degree of accountability placed on those who desire access to the information. Disclosure should be made on a need-to-know basis. There should be a compelling reason to make any information available and that availability should be as restricted as possible.